Título: Esquemas de privacidade nas moedas criptográficas Monero e Zcash
Orientador: Routo Terada
Estudante: André Souza Abreu

INTRODUÇÃO

Nos últimos anos temos presenciado o surgimento de inúmeras moedas digitais baseadas em protocolos criptográficos, a primeira delas sendo o Bitcoin. O Bitcoin é uma forma de dinheiro digital escasso e que não depende de terceiros de confiança, sendo um sistema de pagamentos descentralizado de arquitetura ponto-a-ponto. Em todo sistema há trade-offs, e no Bitcoin não é diferente: a verificação da validade das regras do protocolo é feita utilizando um registro de dados totalmente público, que apesar de ter suas vantagens, também acaba comprometendo, em certo nível, a privacidade dos usuários. Diante disso, outras moedas digitais surgiram com a proposta de permitir um alto nível de privacidade, sem revelar as informações de seus usuários, ao mesmo tempo que mantém um registro de dados distribuído, verificável, e sem necessidade de confiança em terceiros. Neste sentido, as moedas criptográficas que mais tem se destacado são Monero e Zcash.

OBJETIVO

O objetivo deste trabalho é estudar os mecanismos pelos quais estas duas moedas criptográficas proporcionam maior privacidade aos seus usuários: os tipos de privacidade adquirida, o grau de privacidade proporcionado, o funcionamento do sistema do ponto de vista criptográfico-computacional, suas vantagens e trade-offs.

CRONOGRAMA

	ABRIL	MAIO	JUNHO	JULHO	AGOSTO	SETEMBRO	OUTUBRO	NOVEMBRO	DEZEMBRO
Estudar as referências									
Desenvolver a monografia									
Preparar a apresentação									

BIBLIOGRAFIA BASE

[1] Koe; Kurt M. Alonso; Sarang Noether. "*Zero to Monero"*, versão 2.0.0, 2020.

[2] SerHack; Monero Community. "*Mastering Monero: the future of private transactions"*, 1ª Ediçao, 2018.

[3] Sean Bowe, Taylor Hornby, Nathan Wilcox. "*Zcash Protocol Specification*", versão 2022.3.9, 2022.

[4] Paige Peterson; Marshall Gaucher. *"Zcash Documentation"*, versão 5.4.2, 2023.